

A TRUE COPY

Nov 09, 2020

s/ Daryl Olszewski

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)the premises (lower unit, basement and garage)
located at 2718 North 58th Street, Milwaukee, WI
53218, more fully described in Attachment A.

Case No. 20 MJ 222

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Sections 1591, 1594	Sex Trafficking and Conspiracy to Engage in Sex Trafficking
18 U.S.C. Section 1592	Use of Facility in Interstate Commerce, Proceeds of Prostitution
18 U.S.C. Section 922(g)(1)	Unlawful possession of a firearm by a felon (*See Affidavit for additional charges)

The application is based on these facts:

See Attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

TFO Heather L. Spranger, FBI
Printed name and titleAttested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone (specify reliable electronic means).

Date: November 9, 2020

City and state: Milwaukee WI

Judge's signature

Honorable William E. Duffin, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Heather L. Spranger, having been duly sworn, hereby depose and state as follows:

AGENT BACKGROUND AND EXPERIENCE

1. I have been employed with the Racine County Sheriff's Office since 2013 and am currently assigned the rank of Investigator. I am sworn and deputized as a Task Force Officer with the Federal Bureau of Investigation (FBI) and have been assigned to the FBI Milwaukee's Human Trafficking Task Force since December 2019. My duties include investigating violations of federal law, including but not limited to offenses involving the coercion, enticement, and sexual exploitation minors of minors, forced labor, and sex trafficking.

2. I am a law enforcement officer within the meaning of Title 18, United States Code, Section 2510(7), and I am empowered by law to conduct investigations, execute and serve search warrants, and make arrests for offenses enumerated in Title 18 of the United States Code or committed against the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, information obtained from citizen witnesses, and information reported to me by other law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable.

PURPOSE OF THE AFFIDAVIT

4. This Affidavit is made in support of an application for a warrant authorizing the search of the lower unit, basement, and garage of a residence located at **2718 N 58th Street, Milwaukee, Wisconsin 53532** (hereinafter referred to as the "Target Premises"), more particularly described in Attachment A of this Affidavit, and to seize any and all items listed in Attachment B as instrumentalities, fruits, and/or evidence of the criminal activity specified herein.

5. Based on the information set forth in this Affidavit, there is probable cause to believe that at the Target Premises, there exists evidence of violations of Title 18, United States Code, Sections 1591(a)(1)&(b)(1) (sex trafficking by force, fraud, or coercion); 1594 (conspiracy to engage in sex trafficking); 1952(a)(3) (use of a facility in interstate commerce to promote, manage, or carry on unlawful prostitution activity); 922(g)(1) (unlawful possession of a firearm by a person convicted of a crime punishable by imprisonment exceeding one year); 922(g)(3) (possession of firearm by an unlawful drug user), and Title 21, United States Code, Sections 841(a)(1) (manufacture and distribution of a controlled substance).

6. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

PROBABLE CAUSE

7. Case agents have been investigating SAMUEL SPENCER and ERICKA BUIE for using force, fraud, and coercion to cause victims to engage in commercial sex acts. SPENCER is also being investigated for the sale and distribution of various narcotics, as well as being a felon in possession of firearms.

I. Information Provided by Victim 1

8. On August 1, 2016, SPENCER was stopped for a traffic infraction by the Glendale Police Department. He had an active warrant for Battery from the Franklin Police Department and was arrested. The passenger of the vehicle SPENCER was driving was an adult female who will hereinafter be referred to as Victim 1. Victim 1 said she knew SPENCER as “Bin Laden.” She disclosed to Glendale PD that he was forcing her to engage in commercial sex acts and taking all

the profits of such activity. Victim 1 stated that SPENCER would take photos of her and use them to post commercial sex advertisements for her online.

9. Between August 2016 and December 2016, Victim 1 left and returned to SPENCER multiple times, usually coinciding with periods when she was incarcerated. During the periods when she was away from him, she gave multiple interviews to members of the FBI Human Trafficking Task Force about SPENCER.

10. Victim 1 stated that SPENCER controlled when she ate, slept, and performed commercial sex acts. Victim 1 disclosed that SPENCER had other girls who worked for him as well. Victim 1 stated SPENCER would transport her to Iowa and Chicago for commercial sex acts.

11. Victim 1 stated SPENCER instructed her to charge \$250-350 for an hour and \$150-\$200 for a half hour. He also imposed rules for her commercial sex dates, such as no kissing and no anal sex, unless customers were willing to pay extra money. Victim 1 also stated SPENCER would count the condoms he gave her to ensure he was being paid for every date she did.

12. Victim 1 also disclosed that SPENCER admitted to trafficking the daughter of another woman who worked for him. Victim 1 was aware that the girl was only 16 years old at the time. When Victim 1 called him out on trafficking a 16-year-old, SPENCER replied, "Money is money."

13. Victim 1 stated that in addition to trafficking women and girls, SPENCER sold illegal drugs, including heroin, cocaine/crack, and crystal meth. Victim 1 stated that SPENCER used cocaine and would become extremely aggressive when he consumed the drug.

14. Victim 1 stated that SPENCER would “put his hands” on her all the time, meaning that he would cause her physical harm. She stated she once told him that she didn’t need him, and he slapped her in the mouth. Another time, SPENCER beat Victim 1 so severely that she had bone fractures and a broken nose and had to be treated at a hospital. Victim 1 stated that she had heard he also beat the other women and girls working for him, including a white female who was one of the mothers of his children, hereinafter referred to as Victim 2.

15. Victim 1 stated she had become addicted to heroin because SPENCER would provide the drug for her. After a few days of not doing heroin, she would experience withdrawal symptoms such as feeling sick, throwing up, having severe cramps, and having hot/cold sweats. Victim 1 stated there was an incident where Victim 1 became extremely ill due to withdrawal and called SPENCER to bring her more heroin. He stated he would not give her any drugs to make her feel better unless she did a commercial sex act. Victim 1 stated that she did not feel good enough to do a date and stated SPENCER’s response was, “I’m sorry you don’t feel good, but my pockets don’t feel good either.” Victim 1 took this to mean she had to do a date to get the drugs she needed to feel better.

16. Victim 1 also stated that SPENCER would post advertisements for commercial sex acts featuring photographs of her. He paid for these advertisements by using Paypal, Amazon gift cards, or Bitcoins. Victim 1 stated that he used the combination of the nicknames “Bin Laden” and “Ready” in most of the email addresses he used to post on backpage.com (a website that is no longer in operation, but was formerly used to facilitate commercial sex dates). Victim 1 recalled one of the emails used for an advertisement for her posted on Backpage.com by SPENCER was ibenready@gmail and used the associated telephone number 414-552-XXXX.

17. Your Affiant is also aware that on February 25, 2012, the Milwaukee Police Department (MPD) interviewed Victim 1 at Mount Sinai Hospital. Victim 1 had requested to speak with law enforcement about a pimp. During the interview, Victim 1 reported that SPENCER had taken over trafficking her from another pimp around the time of her birthday the previous year, which would have been in September 2011. Officers noted that she had a large scar on her face, and Victim 1 explained that this injury came from Spencer striking her with a belt.

II. Information Provided by Victim 3

18. On July 31, 2020, an adult female herein after referred to as Victim 3 called police to report an armed robbery taking place at 2718 N. 58th Street, Milwaukee, Wisconsin, the Target Premises. Officers of the Milwaukee Police Department (MPD) took an initial report from Victim 3. She stated she was at the above-mentioned address, which she identified as belonging to ERICKA G. BUIE, doing laundry at approximately 6 a.m. Victim 3 stated that she was robbed at gunpoint of \$328 (which she stated was comprised of \$20 bills of U.S. Currency), an LG phone (not activated/no phone number) with nail polish on the back, 20 lottery tickets, a bag of laundry, and a large black purse.

19. Victim 3 stated she knew one of the suspects as “Samuel,” and he was the boyfriend of BUIE. Later that day, Victim 3 identified SPENCER from a photo array as “Samuel.” Victim 3 told MPD that SPENCER also resides in the lower unit at the Target Premises. Victim 3 described the second suspect as a black male with a light complexion known to her as “Nephew.”

20. Victim 3 stated that during the robbery, SPENCER and “Nephew” used force against her without her consent. Both men were armed with firearms during the event, and SPENCER strangled Victim 3 with both hands, impeding her ability to breathe and caused redness,

pain, and swelling to her neck. SPENCER also struck her in the back of the head, causing pain and swelling. SPENCER told Victim 3, "I'm going to shoot you, you bitch." Officers observed visible red marks on her neck.

21. Victim 3 also told officers that SPENCER came from behind her and struck her on the left side of the face with a black and silver handgun. This caused her to fall backwards, and SPENCER jumped on top of her and started to go through her pockets. Victim 3 stated that SPENCER took the \$328 in U.S. Currency that she had in her right pants pocket. She stated that SPENCER still wanted more money and was trying to take her purse. A struggle over the purse ensued which caused Victim 3 to urinate herself out of fear.

22. After SPENCER got off of Victim 3, she attempted to leave the Target Premises, however, SPENCER and "Nephew" stood by the doorway, preventing her ability to leave. Victim 3 stated that "Nephew" was armed with a rifle. Both suspects demanded more money, and SPENCER then physically attacked her. SPENCER pointed his gun towards Victim 3's head and threatened to kill her.

23. Victim 3 then gave SPENCER an old debit card that no longer worked. She stated that "Nephew" took her to an ATM to withdraw money, however she was able to run away and make it back home.

24. The FBI Human Trafficking Task Force conducted a follow-up interview with Victim 3 on August 14, 2020. Victim 3 stated that she knew SPENCER by the following names: "Sam," "Ben," "Bin Laden," "Ben Ready," and "Benjamins."

25. Victim 3 stated that SPENCER mostly sells drugs, including crack, heroin, weed, and ecstasy. Victim 3 also described SPENCER as dangerous to women because he is abusive.

Victim 3 stated that he was physically abusive to Victim 2 and that she had witnessed him break BUIE's nose and ribs. She stated that she also saw SPENCER use physical violence against another white female who worked performing commercial sex acts dates for him.

26. According to Victim 3, the incident on July 31, 2020 at the Target Premises was the first time SPENCER "put hands on her" or threatened her. She stated that her neck was still sore to the touch and it hurt to speak.

27. Victim 3 stated that BUIE posts commercial sex advertisements on the website "xcityguide" for women who come to the Target Premises. Victim 3 stated BUIE also controls and handles multiple phone lines to coordinate the "dates" for the women. Many of these commercial sex dates take place at the Target Premises.

28. Victim 3 also explained to Milwaukee Police Department that BUIE runs a webcam service called "Perfect Bae" from the Target Premises. BUIE sets up webcams in the back bedroom of the Target Premises. This webcam service is intended to record, sell, and distribute erotic videos featuring women.

29. Victim 3 said BUIE's Facebook username is "Purfekt," which she describes as her "nickname." This name is similar to that of BUIE's webcam business.

30. Victim 3 stated that the women who work for SPENCER and BUIE perform commercial sex dates in the basement of the Target Premises. These women enter and exit via the back door (the northeast door) of the residence. This door is also used as used an entrance for the commercial sex customers. It leads directly to the basement of the residence, and it also serves as an entrance for the upper unit. According to Victim 3, there is also a second entrance for the lower unit through this entrance.

31. Victim 3 stated there are typically three to four women in the house (lower unit and/or basement) performing commercial sex acts at a time. The rooms in the basement and rooms in BUIE and SPENCER's unit are where the commercial sex acts occur. Victim 3 described the basement as having four to five rooms that are used for commercial sex acts throughout the day.

32. Victim 3 also said that SPENCER is "known to keep women hostage at that apartment," meaning the lower unit of the Target Premises. Victim 3 stated he does this by threatening them with physical harm and taking their ID's and credit cards. She stated SPENCER keeps these cards in the closet of the bedroom to the right of the bathroom in SPENCER and BUIE's unit. SPENCER also maintains control over women by taking and monitoring their phones.

33. Victim 3 stated that while BUIE manages and posts advertisements for the commercial sex acts that occur at that residence, SPENCER will transport the women to known prostitution tracks on W. Lisbon Avenue and on the southside of Milwaukee. Victim 3 estimated that 10-20 women work for SPENCER off and on at any given time.

34. Victim 3 stated that SPENCER keeps all of the money that women make from commercial sex acts. He compensates the women by feeding them with drugs, or he will sometimes give them \$30-\$40 following one of their dates. Victim 3 explained this would be just enough money to keep the women around and give them ability to purchase drugs, food, or other needs.

35. Victim 3 stated SPENCER controlled her by manipulating her crack cocaine addiction over her. SPENCER would only provide drugs to Victim 3 if she gave him the money

that she earned by performing commercial sex dates. At that time, however she denied that she “worked for” SPENCER or BUIE.

36. The Task Force interviewed Victim 3 again on August 28, 2020. During this interview, Victim 3 admitted that she did perform commercial sex acts SPENCER’s direction. Victim 3 stated that she, along with multiple other women, did commercial sex acts out of the Target Premises. Victim 3 had to pay BUIE and SPENCER \$20 for every date she did there.

37. Victim 3 stated that SPENCER and “Nephew” always carry firearms. SPENCER is a convicted felon. Your Affiant is aware of three prior felony convictions on his record. These include the two most recent convictions: a conviction for Possession with Intent to Deliver Cocaine and a conviction for Possession of a Firearm by Felon from April 28, 2009 under Milwaukee County Circuit Court case number #2008CF005263.

38. According to Victim 3, Spencer keeps a “machine gun” firearm in the kitchen of the residence above the sink. She also stated that there are multiple security cameras both in the interior the lower unit and outside the Target Premises.

39. Victim 3 also stated that SPENCER uses the text application “TextNow” for “everything,” which she described as including selling drugs and advertising women for commercial sex acts.

III. Events of June 9, 2020

40. On June 9, 2020, the MPD District 2 - FBI Southeastern Wisconsin Regional Gang Task Force conducted a traffic stop of a vehicle SPENCER was driving at 1425 W. Greenfield Avenue.

41. SPENCER was found to have a semi-automatic pistol, black in color, Taurus 9mm, with magazine- Serial #TFT59616 in his waistband. Officers also saw him throw, and recovered, multiple, individually-wrapped baggies of what was tested and shown to be cocaine with fentanyl. The total weight of the narcotics recovered was 2.74 grams.

42. On August 9, 2020, a federal Grand Jury sitting in the Eastern District of Wisconsin indicted SPENCER for violations of Title 18, United States Code, Sections 922(g)(1) and 924(a)(2), as well as Title 21, United States Code, Sections 841(a)(1) and 841(b)(1)(c). An arrest warrant was issued on August 11, 2020. See Attachment C.

IV. Commercial Sex Advertisements

43. Case agent located commercial sex act advertisements from the website Skipthegames.com for Victim 2, whom Victims 1 and 3 had witnessed him physically abuse, on Skipthegames.com. The photographs on these advertisements were of Victim 2's face and therefore could be visually identified as her. The advertisements were posted on January 22, 2020 (Post IDs #779714828291 and #397665988935). The email used for both posts was sssir454@gmail.com.

44. The IP addresses used to post the advertisements was 75.10.183.46. This IP address is maintained by AT&T. According to AT&T's records, the subscriber for the IP address on the relevant date and time was ERICKA BUIE, with a listed telephone number of 414-888-XXXX. The billing and service address listed was the address of the Target Premises.

45. Law enforcement also located a commercial sex advertisement from Skipthegames.com for Victim 3 (Post ID #398746030540). This advertisement features photographs of Victim 3 (visually identified as Victim 3 because the advertisement featured a

photograph of her face), along with photos of 10 other females, and was posted on March 28, 2020. The telephone number listed on the advertisement is 414-888-XXXX, the same number associated with the above-discussed AT&T IP address.

46. The email address associated with this ad was purfektbih@gmail.com, which is similar to the name of BUIE's web camera business (PerfectBae.com) and BUIE's Facebook username (Purfekt).

47. The IP address associated with this ad was 75.10.183.46, is the same IP address that was used to post the aforementioned ads posted on January 22, 2020. AT&T records confirmed that BUIE was still the subscriber, with the same contact and location information. Skipthegames.com records show that IP address was used to post more than 300 commercial sex advertisements on their website.

V. Links Between SPENCER, BUIE, and the Target Premises

48. In Milwaukee County case number 2020CF002135, filed on June 12, 2020, SPENCER gave the address of the Target Premises to the Court as his address. This is also the address SPENCER gave MPD at the time of his arrest on June 9, 2020. A CLEAR check of the VIN number of the vehicle SPENCER was driving at the time of his arrest shows that it was registered to ERICKA BUIE at the address of the Target Premises.

49. On August 17, 2020, the FBI Southeastern Wisconsin Regional Gang Task Force conducted surveillance outside of the Target Premises. During the surveillance, Task Force members witnessed SPENCER at the residence. Task Force members also witnessed what, based on their training and experience, they believed to be several hand-to-hand drug transactions taking place in front of the residence.

50. On September 2, 2020, Task Force members again witnessed SPENCER at the residence. There was heavy counter surveillance by “spotters,” which is described by FBI Gang Task Force Agents as potential drug users set outside residence to watch for police and/or other law enforcement entities). Due to this, the Task Force members were unable to follow SPENCER when he left the residence.

51. On November 5, 2020 at 1:10 P.M., the FBI Surveillance Operations Group again witnessed SPENCER at the Target Premises, entering the lower unit.

VI. Training and Experience Regarding Sex Trafficking

50. Through my training, experience, and consultation with other law enforcement officers, I have learned that individuals involved in sex trafficking:

- a. Maintain records, including electronic files, in their residences, related to their illicit business on computers and servers hosting internet applications such as Facebook.
- b. Solicit clients through electronic advertisements and other media.
- c. Commonly earn income in the form of cash and try to legitimize these profits. In order to do this, subjects frequently attempt to transfer and conceal the money by means such as placing assets in names other than their own to avoid detection while maintaining control; hiding money in their homes, safes, and safety deposit boxes; or using the money to buy assets which are difficult to trace. Records of these and other types of transactions are often found at the residences of individuals involved in illicit commercial sex;
- d. Use cellular telephones to promote and carry on their business and maintain these items on their person and/or in their residences.

51. The information set forth above suggests that this general learning and knowledge are true as to SPENCER and BUIE. For example, Victim 3 told FBI Human Trafficking Task Force that SPENCER was continually contacting her over Facebook Messenger Application. BUIE posted advertisements for commercial sex acts for women that allegedly worked for her and

SPENCER on the internet by use of electronic devices (ie-cellular phones, webcam equipment, computers, tablets, etc.). The fact that SPENCER is residing at BUIE's residence and BUIE is described as setting up the commercial sex dates, shows that SPENCER maybe trying to place assets in her name or hid them among her belongings. Victim 3 also stated that BUIE "works the phone." This indicates that BUIE utilizes her cellphone to communicate with potential customers of commercial sex acts.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

52. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **IP Address:** The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. **Storage medium:** A storage medium is any physical object upon which computer data can be recorded. Examples include external hard drives, flash memory, CD-ROMs, and other magnetic or optical media.

53. As described in Attachment B, this application seeks permission to search for records that might be found on the Target Premises, in whatever form they are found. One form in which the records might be found is data stored on a cellular telephone, a computer's hard drive,

or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

54. I submit that if a computer (including a cellular telephone), or storage medium is found on the Target Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

55. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant,

but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Target Premises because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically

also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to post commercial sex advertisements or communicate with prospective commercial sex buyers, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

55. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

56. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably

appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

57. Based upon the information provided above, your Affiant respectfully submits that there is probable cause for the issuance of the requested warrant.

ATTACHMENT A
Premises to Be Searched

The property to be searched is located at 2718 N. 58th Street, Milwaukee, Wisconsin. That address is a two-story, multi-family residence that is divided into an upper and a lower unit. There are two doors that lead out of the interior of the building, both on the east side of the building, adjacent to an alleyway. The portion of the residence at that address to be searched is the lower unit, as well as the shared basement and two-car garage (not attached), including any vehicles parked within it. Additionally, it includes any vehicles parked in the driveway (parking pad) next to the residence that are registered to that address, including a 2007 blue Buick Lacrosse bearing Wisconsin license plate AGK7792.





ATTACHMENT B
Items to Be Seized

All evidence, instrumentalities, information, records, physical items, and contraband relating to violations of Title 18, United States Code, Sections 1591(a)(1)&(b)(1) (sex trafficking by force, fraud, or coercion); 1594 (conspiracy to engage in sex trafficking); 1952(a)(3) (use of a facility in interstate commerce to promote, manage, or carry on unlawful prostitution activity); 922(g)(1) (unlawful possession of a firearm by a person convicted of a crime punishable by imprisonment exceeding one year); 922(g)(3) (possession of firearm by an unlawful drug user), and Title 21, United States Code, Sections 841(a)(1) (manufacture and distribution of a controlled substance) for the period of September 1, 2011 through the present, including:

1. Any and all records and information reflecting, referring, indicating, or in any way relating to ownership, occupancy, residency, or rental of the premises;
2. All items commonly associated with use for commercial sexual activity, such as condoms, sexual lubricants, and clothing or undergarments used for stripping and exotic dancing;
3. Any notes, documents, records, or correspondence, in any format or medium, concerning communications between individuals about commercial sex acts or sex trafficking, or advertisements for the same, such as on Skipthegames.com, Backpage.com, and similar websites;
4. Any and all surveillance video and/or audio recordings, recording equipment, web camera equipment, and monitors, and any records relating to the purchase, use, installation, or operation of such systems;
5. All financial records, including but not limited to ledgers, account books, appointment books, tax returns, tax return information, checks, checkbooks, bank statements, loan records, receipts, bills, invoices, credit card receipts, contracts, leases, and related correspondence;
6. Any credit cards, debit cards, gift cards, prepaid cards, state identification cards, driver's license cards, passports, and/or belongings of females other than Ericka BUIE;
7. Firearms, ammunition, magazines, attachments, or cases, as well as and any related manuals or ownership documentation; and
8. Indicia of unlawful possession, use, or distribution of controlled substances, including but not limited to paraphernalia and evidence known to be associated with drug trafficking and/or drug possession.

9. For any computer or electronic storage medium located on the premises that contains any of the above records or information:

- a. Evidence of who used, owned, or controlled the computer or electronic storage medium at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. Evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;
- c. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- d. evidence of the absences of such malicious software;
- e. evidence indicating how and when the computer was accessed or used to determine the chronological context of access, use, and events relating to the crime under investigation and the computer user;
- f. Passwords, encryption keys, and other access devices that may be necessary to access the computer or storage medium;
- g. records of or information about Internet Protocol (IP) addresses used by the computer;
- h. records of any GPS or other location information generated by or stored on the computer;
- i. records of or information about the computer’s internet activity, such as firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- j. Documentation and manuals that may be necessary to access or to conduct a forensic examination of the computer or storage medium; and
- k. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

As used above, the term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

As used above, the term “electronic storage medium” includes any physical object upon which computer data can be recorded. Examples include external hard drives, flash memory, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the
Eastern District of WisconsinUnited States of America
v.SAMUEL L. SPENCER
Defendant)
)
)
)
)
)
)

Case No. 20-CR-142

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay
(name of person to be arrested) SAMUEL L. SPENCER,
who is accused of an offense or violation on the following document filed with the court:

- ☒ Indictment ☐ Superseding Indictment ☐ Information ☐ Superseding Information ☐ Complaint
☐ Probation Violation Petition ☐ Supervised Release Violation Petition ☐ Pretrial Release Violation Petition
☐ Violation Notice ☐ Order of Court

This offense is briefly described as follows: 18 USC § 922(g)(1) and 924(a)(2) – Unlawful Transport of Firearms

Date: August 11, 2020

GINA M. COLLETTI, Clerk, U.S. District Court

City and State: Milwaukee, WisconsinBy: K. Hubacz, Deputy Clerk*Printed name and title***Return**

This warrant was received on (date) _____, and the person was arrested on (date) _____
at (city and state) _____.

Date: _____

*Arresting officer's signature**Printed name and title*

U.S. DISTRICT COURT
EASTERN DISTRICT - WI
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN
2020 AUG 11 A 11:30

UNITED STATES OF AMERICA, **CLERK OF COURT**

Plaintiff,

v.

SAMUEL L. SPENCER,

Defendant.

20-CR-1421

Case No. 20-CR

[18 U.S.C. §§ 922(g)(1) & 924(a)(2);
21 U.S.C. §§ 841(a)(1) & 841(b)(1)(C)]

INDICTMENT

COUNT ONE

THE GRAND JURY CHARGES THAT:

1. On or about June 9, 2020, in the State and Eastern District of Wisconsin,

SAMUEL L. SPENCER,

knowing he previously had been convicted of a crime punishable by imprisonment for a term exceeding one year, knowingly possessed a firearm which, prior to his possession of it, had been transported in interstate commerce, the possession of which was therefore in and affecting commerce.

2. The firearm is more fully described as a Taurus, model PT 24/7 G2C, 9mm pistol, bearing serial number TFT59616.

All in violation of Title 18, United States Code, Sections 922(g)(1) and 924(a)(2).

COUNT TWO

THE GRAND JURY FURTHER CHARGES THAT:

On or about June 9, 2020, in the State and Eastern District of Wisconsin,

SAMUEL L. SPENCER

knowingly and intentionally possessed with intent to distribute a controlled substance, namely, a mixture and substance containing cocaine base, a Schedule II controlled substance, and a mixture and substance containing cocaine, a Schedule II controlled substance.

In violation of Title 21, United States Code, Sections 841(a)(1) and 841(b)(1)(C).

A TRUE BILL:

[REDACTED]

FOREPERSON

Date: 8/11/20


MATTHEW D. KRUEGER
United States Attorney